

Perancangan Kriptografi *Block Cipher* Menggunakan Pola Bentuk Tubuh Hewan Laut (Kura-kura, Kepiting, Lobster, Ikan Pedang)

Satria Bagaskara¹, Eko Sedyono²

Fakultas Teknologi Informasi

Universitas Kristen Satya Wacana

Jl. Diponegoro 52-60, Salatiga 50711, Indonesia

E-mail: 672013013@student.uksw.edu¹, ekosed1@yahoo.com²

Abstract

Cryptography is a technique of securing data. To improve the security level, cryptography needs to be developed. Block Cipher cryptography using the pattern of Body Shape of Marine Animals (Turtle, Crab, Lobster, Marlin) is designed with block size as much as 64 bits to create new cryptography. This cryptography is designed using 4 process and 20 rounds, where the 2nd and 3rd processes are transformed using the s-box table to get more random Ciphertext. Testing is also done using Avalanche Effect and Correlation value where character changes reach 48.98437%, so it can be used as an alternative in securing data.

Keyword : *Block Cipher, Cryptography, Marine Animals, Avalanche Effect, S-Box.*

Abstrak

Kriptografi adalah teknik mengamankan data. Untuk meningkatkan keamanan, kriptografi perlu dikembangkan. Kriptografi *Block Cipher* menggunakan pola Bentuk Tubuh Hewan Laut (Kura-kura, Kepiting, Lobster, Ikan pedang) ini dirancang dengan ukuran blok sebanyak 64 bit untuk membuat kriptografi baru. Kriptografi ini dirancang menggunakan 4 proses 20 putaran, dimana proses ke-2 dan ke-3 ditransformasikan menggunakan tabel *S-Box* untuk mendapatkan *Ciphertext* yang lebih acak. Pengujian juga dilakukan menggunakan *Avalanche Effect* dan nilai Korelasi dimana terjadi perubahan karakter mencapai 48.98437%, sehingga dapat digunakan sebagai alternatif dalam mengamankan data.

Kata Kunci : *Block Cipher, Kriptografi, Hewan Laut, Avalanche Effect, S-Box.*

¹⁾ Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana

²⁾ Staff Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana Salatiga